

Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide

by Christopher Wolf
Directors, Privacy and Information Management Practice
Hogan Lovells US LLP
christopher.wolf@hoganlovells.com

In this computerized and inter-connected era, companies hold and exchange vast amounts of personal data relating to employees and consumers. Whether a company obtains that data from other companies in its role as a service provider or database manager, or whether it is the “owner” of the data, it is now well understood that companies that collect, maintain, or use personal information have a serious responsibility to protect the security and integrity of that information.

The unwanted release or exposure of personal information can intrude upon privacy and lead to harm such as identity theft. That is why lawmakers, regulators, and advocates worldwide recently have focused significant attention on data security and data security breaches. The potential exposure from breaches is great and data security is becoming a major risk management priority. While this document does not address data security safeguards, the model security breach response plan is intended to compliment a company’s data security program designed to ensure that appropriate protections are in place, including administrative (policies and procedures), physical (secure facilities and paper files) and technical (encryption, firewalls, etc.) safeguards. Despite safeguards, it is important to plan for a Security Breach because even with reasonable protections in place, data breaches occur. Breaches can result in huge expenditures for remediation and in harm to a company’s reputation of trust.

The specific legal obligations started in California in 2003, when that state’s law began to impose an obligation on those holding personal information to provide notice if there is a breach of the security of that information. Most US jurisdictions require such notification, and there are many variations within the state statutes in what triggers a notice, what goes in the notice, who gets notified, when the notices should go out, and more. In addition, the federal government recently legislated with respect to notices following the breach of health data and both the Federal Trade

Commission and Department of Health and Human Services have enacted notification rules that have implications for HIPAA-covered business associates and other service providers handling health data. Significantly, the Federal Trade Commission, State Attorneys General, and private plaintiffs have pursued companies large and small that have suffered data security breaches. Their focus has been not only on whether the notice protocols have been followed but also on the underlying data security at the company. All of this means that how a company responds to a data security breach is increasingly important.

What follows is a model data security breach preparedness guide designed to facilitate compliance with legal obligations and to address reputational issues. This is not a “one-size fits-all” guide that applies to all companies, but is intended to illustrate what a typical preparedness plan looks like. It also is not intended to constitute legal advice, which only can be provided pursuant to a duly-confirmed attorney-client relationship.

THE DO’S AND DON’TS OF RESPONDING TO A BREACH

Do’s:

- Have a written post-breach response plan ready and tested *before* a breach happens
- Identify a breach response team and make sure people know what role they will play when a breach happens
- Have a communications plan regarding the breach
- Know what regulations, statutes and contracts cover your post-breach obligations
- When a breach happens, pull out the stops to prevent further exposure of data
- Find out what happened as soon as possible and preserve the evidence
- Contact your insurance carrier and seek legal advice regarding whether the breach triggers notifications requirements and whether those notification requirements apply to your company
- Involve technology and legal experts as needed
- Have draft model notices ready to be customized depending on the facts
- Contact law enforcement, credit reporting agencies, and as needed
- Keep regulators informed where required by law and were appropriate – if they are surprised, they will not be happy

Don’ts:

- Don’t delay in providing notices when legal counsel determines they are required or advisable – the time deadlines are strict
- Don’t communicate with the public about the breach until you know the fundamental facts
- Don’t ignore your important business customers and partners – keep them informed
- Don’t necessarily accede to every demand from a business customer and partner –weigh demands carefully in light of your total response plan
- Don’t skimp in providing help to consumers – their goodwill could forestall legal difficulties
- Don’t forget to update your post-breach response plan regularly

Hogan Lovells' Model Data Security Breach Preparedness Guide

Actions at the Time of a Data Security Breach

A. Steps for Immediate Mitigation and Incident Analysis.

1. Contain Data Security Breach.
 - a. For breach involving electronic data:
 - i. Implement Electronic Incident Response Plan.
 - b. For non-electronic data or physical breach:
 - i. Promptly investigate incident and take steps necessary to limit further data loss.
 - ii. Immediately secure physical area; change locks, access codes, or cards, if necessary.
 - iii. Determine whether it is appropriate to involve law enforcement.
 - iv. Limit traffic into affected area until Corporate Security and/or law enforcement has investigated.
 - v. If media, paper, or other physical data assets were lost by vendor, obtain tracking information, video monitoring, if available.
 - vi. Determine measures needed eliminate vulnerability and prevent recurrence.
2. Convene the Information Security Steering Committee and/or the Security Breach Response Team as necessary.
 - a. The Information Security Steering Committee (ISSC) should jointly be involved in the initial steps set forth in Section A.1 above.
 - b. If after its initial assessment, the ISSC determines this may be a Data Security Breach involving personal information, the ISSC shall ensure that all representatives on the Security Breach Response Team are aware of the incident. Communications should be made by telephone where possible to prevent vital communications from leaking if email systems are compromised.
 - c. Individual members of the Security Breach Response Team will inevitably vary depending on the specific breach that arises. However, the standing Security Breach Response Team should include, at a minimum, representatives from the following areas:
 - i. Office of General Counsel
 - ii. Data Office (if applicable)
 - iii. Corporate Security
 - iv. Information Security
 - v. Human Resources
 - vi. Internal Audit
 - vii. Office of Media Relations
 - d. The current members of the standing Security Breach Response Team are listed on Annex I.
 - e. In the event of a Data Security Breach involving _____ computer systems, the Security Breach Response Team shall include appropriate members as identified in the Electronic Incident Response Plan.
3. Analyze the Data Security Breach.
 - a. Record all information relevant to breach.
 - i. All available data related to the breach should be collected at the direction of counsel so that the information can be analyzed to determine necessary remediation steps and legal responsibilities, and can be provided to assist law enforcement investigations resulting from the breach. Identify member of Security Breach Response Team with responsibility for leading this effort. **[Mark all written reports with the following notice: "Privileged and Confidential: Attorney-Client Privileged Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice."]**
 - ii. Information that should be captured and recorded is listed on Annex II.
 - b. Analyze the immediate ramifications of the breach.

Information to be Collected Immediately Following Data Security Breach

1. Date, time, duration, and location of breach.
2. How the breach was discovered, by whom, and any known details surrounding the breach (e.g., method of intrusion, entry or exit points, paths taken, compromised systems, whether data was deleted vs. modified vs. viewed, whether any physical assets are missing).
3. Details about the compromised data, including a list of affected individuals and type (employee, vendor, customer, etc.), data fields (including all fields of personal information maintained), number of records affected; whether any data was encrypted (if so, which fields), and what customer the data relates to.

If unencrypted name plus Social Security number, driver's license or state ID, credit card or bank account information with PIN or password was compromised, immediately notify Security Breach Response Team.

- i. Evaluate and understand the cause of the incident.
 - ii. Identify who the affected persons are and what Personal Information has been compromised.
 - iii. Determine what is likely to happen to the data that was compromised.
 - iv. Determine whether other systems are under threat of immediate or future danger.
 - v. Analysis of a Data Security Breach may involve issues that require the assistance of specialized consultants. If necessary, contact previously identified third party Information Technology consultants to assist in capturing relevant information and performing forensic analysis.
4. Analyze Legal Implications of the Breach.
- a. In conjunction with the general analysis conducted above, conduct specific analysis of legal issues stemming from breach. Legal analysis should include at least the following issues:
 - i. Litigation risk. Review customer, supplier, and any other relevant company agreements, including website privacy policies, to see if company owes notification or other obligations to any third party with respect to data breached.
 - ii. Statutory notification requirements.
 - 1. Identify Legal Jurisdictions Involved. Identify states and/or countries potentially involved in the breach by determining location of the customers, employees, and/or systems affected by the Data Security Breach.
 - 2. Identify Statutes Triggered. Identify federal, state, and international statutes and regulations potentially triggered or violated by the Data Security Breach. Identify the following information within the triggered laws:
 - a. Type of Data: Determine whether compromised Personal Information would trigger data breach notification laws. Generally, notification could be required where the compromised data is unencrypted and includes affected persons' first and last names plus one of the following: Social Security number, drivers license number, state identification number, credit card number, or bank account information with password.
 - b. Jurisdiction: Determine whether, if acting as a service provider to another business, whether notification obligations to such other business have been triggered and if so, whether that satisfies all notification obligations.
 - c. Jurisdiction: Determine whether applicable state or foreign law requires additional consumer notification.
 - d. Law Enforcement Notification Requirement: Determine whether law enforcement or other agencies *must* be notified by law, e.g., states such as Connecticut, Indiana, New Hampshire, New York, New Jersey, North Carolina, Hawaii.
 - e. Notify Credit Agencies: Determine whether credit reporting agencies *must* be notified by law.
 - f. Applicability of specific federal or foreign law: Determine applicability of legislation such as HIPAA (as amended by the American Recovery and Reinvestment Act of 2009), especially if the breach involves health records, and/or member state laws implementing the EU Data Protection Directive.
 - iii. Insurance coverage. Review company's insurance coverage to determine whether breach incident is covered by policy.
 - iv. Indemnification by and/or responsibility of third parties if they are the cause of breach. Analyze and determine whether any third parties have obligations to the company based on their actions or inactions giving rise to the breach.
 - v. Law enforcement investigation of the company. See below for details.
 - vi. Liability of individual employees. Analyze whether employee(s) violated company policies or laws and are responsible for the breach.
 - b. At any point in the process above, in-house counsel shall determine whether to contact outside legal counsel for assistance.
5. Contact Law Enforcement.
- a. Analysis of the compromised data will suggest which legal jurisdictions may be relevant in the event of a Data Security Breach. If necessary, contact the appropriate local and/or federal law enforcement agencies to enable immediate deployment of investigative capabilities. Assign one member of the Security Breach Response Team with responsibility for interfacing with law enforcement agencies. Federal law enforcement contacts are listed on Annex III. Contact information for state regulatory and law enforcement agencies in those jurisdictions where governmental notice is required (if individual notice is required) is provided in Annex IV. Contact information for the three credit reporting bureaus is provided in Annex V. **Note:** It may be appropriate to contact local and or state law enforcement agencies prior to determining whether individual notice is required, which would not implicate Annex IV or Annex V.
 - b. Law enforcement authorities may require a delay in notification to affected persons or release of public information if such activities would hamper law enforcement investigations.
 - c. Local and/or federal law enforcement authorities may desire to conduct an investigation into the company's security systems and response to the Data Security Breach as a part of their investigation of

the incident. Consult legal advisors before notifying law enforcement in order to determine appropriate response to law enforcement inquiry.

- d. Even if no state notification law applies and no inquiry is expected, consider whether a police report should be filed to report the incident (e.g., stolen laptop or burglary on premises).
6. **Contact Insurance Carrier.** Review insurance coverage pertinent to the Data Security Breach and notify the insurance carrier in accordance with policy requirements. (Office of the General Counsel input should be sought before this occurs).
7. **Organize Inquiry Response System.** Depending on the size of a breach and the number of individuals affected, a significant volume of inquiries may be sent to the company in the wake of a Data Security Breach and ensuing individual notification efforts. The company should design a system for handling inquiries before the occurrence of a breach. System design should address the following issues:
 - a. Mode of communication with public (1-800 number, email address);
 - b. Mode of communication with employees;
 - c. Mode of communication with business customers (if holding personal data on behalf of other business as a service provider);
 - d. Training/hiring of Customer Service Representatives to staff inquiry response or outsourcing call center activities; and
 - e. Documentation of inquiry responses, preparation of script; preparation of website Frequently Asked Questions (FAQs). FAQs can be a useful reference for affected individuals and can help to reduce the number of calls to a call center.
8. **Investigate Remediation Strategies.**
 - a. The company may want to offer certain remediation services to assist affected persons following a Data Security Breach. The following strategies could be implemented as appropriate following the occurrence of a breach:
 - i. Credit monitoring services;
 - ii. Identity theft insurance;
 - iii. Identity theft help information packets; and/or
 - iv. Compensation for identity theft.
 - b. A brief discussion of each of the preceding options may be found at Annex VI.

B. If Acting as Service Provider to Another Business for Whom Personal Data is Held, Develop Notification Plan for Business Customer

1. When required or desirable, develop a notification plan for business customers based on requirements of law and contract.
2. Utilize individuals within organization who act as primary contacts for business relationships to make initial contacts to help facilitate the process.
3. Determine the mode of communication for delivering notice, which, in the business customer context is frequently done in-person or by telephone, with a follow-up communication in writing.
4. Expect and anticipate demands that business customer may make, including demands to provide individuals notifications on the business customer's behalf, even if not required by statute or contract. Where not required, business considerations may still dictate providing notifications to affected individuals on behalf of business customers.

C. Develop Notification Plan for Affected Persons.

1. When required or desirable, develop a notification plan for affected persons based on requirements of law and contract.
2. Prepare list of persons to be notified in accordance with statutes and regulations analyzed above. In some cases, the law may not require notice, but the company may decide based on the facts and circumstances of a particular incident to provide notification. The notification plan in any event should be the same.
3. Minimize false-positives, i.e., persons who are accidentally notified but do not fall within the groups of persons intended by the company to be notified.
 - a. Record the process for determining persons to be notified.
4. Determine the mode of communication for delivering notice.

- a. Regulations and prior contractual agreement between the parties may require certain modes of communication.
 - b. In some jurisdictions, the prior consent of affected persons may be required in order to use email notification.
5. The content of notice to affected persons may be dictated by regulation or contract, but notice should generally include the following information:
 - a. Description of what happened;
 - b. Type of protected data involved;
 - c. Actions to protect data from further unauthorized access;
 - d. What the company will do to assist affected persons;
 - e. What affected persons can do to assist themselves;
 - f. Contact information for company inquiry response system (a toll free 1-800 number should be provided); and
 - g. Contact information for local and federal government information.
 6. Sample notice forms for notice to affected persons, as well as notice to credit agencies and media statements may be found at Annexes VII and VIII.
 7. A summary of the special notification provisions required by certain jurisdictions (Maryland, Massachusetts, and Puerto Rico) is provided at Annex IX.

Statutory Data Breach Notification Requirements

- **Identify Legal Jurisdictions Involved.** Identify the states and countries potentially involved in the breach by determining location of the customers, employees, and systems affected by the breach. In the U.S. forty-five states and Washington, DC, the Virgin Islands and Puerto Rico have such laws and there are now federal rules by the Federal Trade Commission and Health and Human Services relating to health information and vendors.
- **Identify Statutes Triggered.** Identify federal, state, and international statutes and regulations potentially triggered or violated by the breach. Identify the following information within the triggered laws:
 1. Type of Data: Determine whether compromised personal information would trigger data breach notification laws. Generally, notification could be required where the compromised data is unencrypted and includes affected persons' first and last names plus one of the following: Social Security number, drivers license number, state identification number, credit card number, or bank account information with password.
 2. Determine whether business customers must be notified.
 3. If assuming your customer(s)' notification obligations, notify law Enforcement, regulators and credit reporting agencies.
 4. Additional federal or foreign laws: Determine the applicability of other legislation such as HIPAA (as amended by the American Recovery and Reinvestment Act of 2009) and/or member state laws.

D. Communications Steps.

1. Internal Communications.
 - a. Implement an internal communications strategy sensitive to possible compromise of typical internal communications systems such as email.
 - b. Reissue a policy statement to employees regarding external communication with media or third parties.
2. Create Communications Strategy.
 - a. Affected Person Notification.
 - i. Notification should be provided according to legal requirements and plan outlined above.
 - ii. Update and revise draft notification form provided at Annex VIII.
 - b. Credit Agency Notification.
 - i. Update and revise draft notification form provided at Annex VII.
 - c. Media and Web Statement.
 - i. Draft media and web statement and/or press release based on incident-specific facts.
 - d. Law Enforcement Notification.
 - i. Law enforcement may require that notification of media or affected persons be delayed to allow time for law enforcement investigation.

3. Preparation of Support Systems.
 - a. Ensure the following systems are operational prior to executing communications strategy:
 - i. Company inquiry response system (as described above).
 - ii. Remediation strategies.
 - iii. If needed, an appropriate mailing vendor(s) is in place and ready to execute.
 - b. Notify credit reporting agencies prior to large notification of affected persons, and/or as required by applicable law, in order to allow agencies to prepare for response.
4. Execute Communications Strategy.
 - a. The Office of Media Relations representative should ensure timely, coordinated execution of external communications.
 - b. Document response to early communications and tailor continuing communications to key audiences as necessary.
5. Handle Follow-up Communications/Returned Individual Notice Mailings
 - a. Collect all returned mailings (e.g., address undeliverable).
 - b. If a large breach, process returned mailings on a rolling basis as follow:
 - i. Maintain database of returned mailings and enter date of return by individual.
 - ii. Run returned mailings through a National Change of Address (NCOA) vendor.
 - iii. Re-mail if new address is obtained.
 - iv. For further returns or if new address is not obtained through NCOA process, take further step of running through a third-party data vendor (e.g., Acxiom and others).
 - v. Track all further returned mails and enter into database.

Actions Following a Data Security Breach (after investigation and notifications have been made)

1. **Implement Remediation Measures.** In accordance with prior arrangements for remediation and information provided in the notice to affected persons, implement appropriate remediation, which may include the following options, discussed further in Annex VI:
 - a. Credit monitoring services;
 - b. Identity theft insurance;
 - c. Identity theft help information packets/letters; and/or
 - d. Compensation for identity theft.
2. **Preparation for Litigation.** Consider litigation matters that may arise, including:
 - a. Civil lawsuits instituted by affected persons against the company;
 - b. Investigation of the company and/or specific employees by law enforcement authorities; and/or
 - c. Indemnification by third parties in the event that third parties are at fault for data security breach.
3. **Security (both Information Technology Systems and physical Security).**
 - a. Conduct full analysis of the Data Security Breach to determine root causes.
 - b. Review applicable access controls and procedures (both before Data Security Breach and those put in place as the result of containment efforts) to ensure that weaknesses have been addressed and resolved.
4. **Operational Controls.**
 - a. Assess operations to determine necessary revisions to data collection, retention, storage, and processing policies and procedures.
 - b. Assess need for additional employee training in data protection policies and processes.
 - c. Review contract provisions (standard and actual) with third parties that handle Personal Information.
 - d. Review relevant website privacy notices and terms of service; update as needed.
 - e. Review relevant agreements with individuals; determine whether form agreements need to be updated.
5. **Assess Effectiveness of Security Breach Response**
 - a. Review steps taken by Data Owners and Security Breach Response Team during the course of the response to the Data Security Breach.
 - b. Implement changes in Security Breach Response Plan to improve effectiveness in preventing and responding to Data Security Breaches.